

National Medical Review Offices, Inc.

5900 Wilshire Blvd., 22nd Floor
Los Angeles, CA 90036

FAX

To: WCC-3
Company:
Re:
FAX: 310-996-3359
cc:

Date: 6/30 2000
Number of pages including cover: 5

From:
National Medical Review Offices, Inc.
5900 Wilshire Blvd., 22nd Floor
Los Angeles, CA 90036
Phone:
FAX:

b6
b7C

C:\Program Files\Microsoft Office\Templates\Letters & Faxes\FAX from .dot

If you do not receive all pages, please contact

b3
b6
b7C
b7E

SEARCHED INDEXED
SERIALIZED FILED
JUL 2 2000
FBI - LOS ANGELES

001261

~~Confidential~~

Page 2 of 4

06/30/00

We believe that [] is a clue evidencing identity of the hacker, because

[]

b6
b7C

6. An investigation of the breach was conducted. This report was prepared by []

[] discovered that password cracking software had been installed on our terminal servers by []

Investigation of Network Security Breach, NMRO – 6/17/2000

Results of the Investigation

I believe the Lophtcrack software was used to gain access to NMRO administrative passwords. Once the malicious user had access to these passwords, they had access to the entire NMRO domain. The hacker logged onto the NMRO domain, as [] and created an email mailbox using [] username/password. The user then gained access to [] email. [] retains copies of his email on the Microsoft exchange server, a malicious user would be able to read and access his mail. This would explain why [] are receiving email that has already been accessed.

b6
b7C

Chronology of Facts

Saturday 6/17/2000

Contacted by [] concerning email security 6/17/2000. Someone from within or outside the NMRO organization is accessing and forwarding email from [] exchange mailboxes.

b6
b7C

~~Confidential~~

Page 3 of 4

06/30/00

Monday 6/19/200

Arrived NMRO at 7:30 am and met with [redacted] briefly concerning the email security incident. [redacted] met with [redacted] [redacted] behind closed doors about the incident.

b6
b7C

[redacted] immediately began to investigate the incident. These were our finding:

1. Someone had tampered with Windows NT Users and Groups permissions on the NMRO primary domain controller other than the authorized network security personnel.

A user account that was disabled by [redacted] after the individual left the company was enabled. The user was our [redacted] After further investigation, several other users and groups have received domain administrator privileges not authorized by the Network Administrator Refer to the NMRO Security Update document for further reference.

b6
b7C

2. [redacted] immediately revoked Admin privileges for all unauthorized users and groups and from the NMRO domain controllers and revoked remote access privileges to the [redacted] is the only NMRO employee that has remote access to the NMRO domain.
3. Focusing our attention on NMRO terminal servers, we discovered Lophtcrack 2.5 software (www.l0pht.com/l0phtcrack/) had been installed on Terminal Server (Frame 2). This software when placed and executed on a Windows NT server will crack all administrative and user passwords. A malicious hacker uses this software to gain password access in the domain. The Lophtcrack folders were deleted off the terminal servers yet the software was not removed properly from the ADD/Remove programs options in the Windows NT control Panel. Therefore leaving a trail that the software was loaded on the server.

~~Confidential~~

Page 4 of 4

06/30/00

4. Upon further investigation Lophtcrack 2.5 was brought into the organization by our [REDACTED]

b6
b7C

[REDACTED]

END OF REPORT

Please call me, or [REDACTED] as soon as possible. Thank you in advance for your attention to this matter.

b6
b7C

Sincerely,

[REDACTED]

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 07/19/2000

[redacted] was interviewed telephonically at [redacted]. After being advised of the official identity of the interviewing agent and the purpose of the interview, [redacted] provide the following information:

b6
b7C

[redacted] is employed by National Medical Review Offices (NMRO) as [redacted] has examined NMRO's event logs and security logs in an attempt to identify the origin of the intrusions into NMRO's computer system between April and June of 2000. [redacted] could not identify a specific user responsible for these intrusions.

[redacted] access to NMRO's system was disabled after his termination. [redacted] subsequently examined the accounts of a number of people who are no longer employed by NMRO. Access to these accounts should have been disabled. However, on approximately 06/15/2000, [redacted] found that the passwords and remote logon capabilities for approximately six of these accounts had been enabled. This included [redacted] account. The majority of these had administrative privileges. These accounts would have to have been enabled from inside the company. However, it is difficult to determine how and when these accounts were enabled.

b6
b7C

There were several instances between the middle of April, 2000 and June, 2000 when NMRO's system had suspicious outages and went down. The system was down for a total of approximately three days. [redacted] suspected that someone was hacking into NMRO's system in an attempt to shut it down.

The affected machine was NMRO's mail server. The intruder may have gained access through a program or batch file on the server. [redacted] and would have had ample opportunity to install such a program on that server.

LOPHT is a hacker group that does not engage in criminal activity. This group created a program called LOPHTCRACKER that cracks system passwords. In [redacted] told [redacted] to run this program on NMRO's system in order to test the system.

Investigation on 07/13/2000 at Los Angeles, California (telephonically)

File # [redacted] Date dictated 07/19/2000

by SA [redacted] *ZB*
ceb

b3
b6
b7C
b7E

To: NSD

From: Los Angeles

Re: [REDACTED] Date 07/20/2000

b3
b6
b7C
b7E

these accounts had been enabled. This included [REDACTED] account. The majority of these had administrative privileges. These accounts would have to have been enabled from inside the company. However, it is difficult to determine how and when these accounts were enabled.

There were several instances between the middle of April, 2000 and June, 2000 when NMRO's system had suspicious outages and went down. The system was down for a total of approximately three days. [REDACTED] suspected that someone was hacking into NMRO's system in an attempt to shut it down.

The affected machine was NMRO's mail server. The intruder may have gained access through a program or batch file on the server. [REDACTED] and would have had ample opportunity to install such a program on that server.

LOPHT is a hacker group that does not engage in criminal activity. This group created a program called LOPHTCRACKER that cracks system passwords. In [REDACTED] [REDACTED] told [REDACTED] to run this program on NMRO's system in order to test the system.

b6
b7C
b7E

[REDACTED] of NMRO's servers which are main domain controllers are named [REDACTED] The Internet Protocol (IP) addresses for these servers are [REDACTED] respectively.

Given that there has not been a verifiable financial loss to NMRO or theft of trade secrets, and because the intrusions are not ongoing, writer recommends that case be opened and closed. Investigation at Los Angeles complete.

\$1 1/2 mil contract
(expected value)

4

Mail to end ~~4/00~~ ~ 6/15 - noticed
acts enabled

[redacted] rights to system re enabled after
[redacted] 2 - 2 1/2 weeks after
[redacted] left to when disabled acts.

b6
b7C

- Mail server affect; suggested - no commands -
made a small or path file [redacted] was

[redacted] had couple of to instal
that software

- LOPHT - Clean hairy group - One of
the profs LO PHT CRACKER for PWS -
[redacted] mentioned that he had that prog -
told [redacted] to run it to test the
system [redacted]

b6
b7C

Log words available

Comp server - Would have log

b7E

[redacted]

Several incidents from mail 4/2000 to mail 6/2000,
significant delays - down, 3 days